Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003	)	CG Docket No. 04-53
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	

COMMENTS OF THE CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION

Howard J. Symons
Angela F. Collins
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004
(202) 434-7300

Michael F. Altschul
Senior Vice President and General Counsel
CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION
1400 16th Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 785-0081

Of Counsel

April 30, 2004

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003	)	CG Docket No. 04-53
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	

COMMENTS OF THE CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION

Pursuant to Section 1.415 of the Commission's rules,[1/] the Cellular Telecommunications & Internet Association ("CTIA") hereby submits its Comments on the Commission's *Notice of Proposed Rulemaking* ("*Notice*") issued in the above-referenced matter[2/] to implement the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act" or "Act").[3/]

INTRODUCTION AND SUMMARY

Congress recognized that unsolicited electronic mail from unknown senders places substantial burdens on consumers, businesses, and Internet access providers. As a result, the CAN-SPAM Act provides consumers with the ability to stop receiving all forms of unwanted messages and gives Internet access providers and state and federal officials the necessary tools to combat unwelcome messages. Specifically, the CAN-SPAM Act requires commercial electronic

---

1/ 47 C.F.R. § 1.415.

2/ *Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*; *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Notice of Proposed Rulemaking and Further Notice of Proposed Rulemaking, 19 FCC Rcd 5056 (2004) ("*Notice*").

3/ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) ("CAN-SPAM Act").

mail messages to include certain information and give consumers the opportunity to "opt-out" of receiving future messages from that sender.[4/]

Congress, however, realized that wireless spam is even more problematic than spam to a desktop computer because wireless spam "follows you wherever you go."[5/] Thus, Congress enacted Section 14 of the Act, which provides wireless subscribers with additional protections from unwanted messages and puts in place more stringent requirements for spammers sending messages to wireless subscribers. Unlike the opt-out mechanism contained in the Act's general provisions, Section 14 adopts more restrictive standards for wireless spam and requires senders to first have a recipient's express prior authorization before sending the message.[6/] Section 14 also demonstrates Congress's recognition that messages sent to wireless subscribers may be unable to comply with the Act's general requirements given the unique characteristics of wireless devices and directs the Commission to consider modifications as necessary to account for such characteristics.[7/]

Like Congress, commercial mobile radio service ("CMRS") providers understand that spam threatens the value of wireless messaging, and therefore, have a strong interest in protecting their customers from unwanted messages. To capture the huge potential of wireless data services, carriers must convince customers to upgrade to handsets and devices that support these services and features, and then to use these services. If spam ruins the user experience, the opportunity of wireless data will be lost. Consequently, many wireless providers have taken advantage of existing technologies and blocking techniques to protect their subscribers from

---

4/ CAN-SPAM Act, § 5.

5/ 149 CONG. REC. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey).

6/ CAN-SPAM Act, § 14(b)(1).

7/ CAN-SPAM Act, § 14(b)(4).

unwanted messages. The CAN-SPAM Act provides additional tools for the prevention of unsolicited wireless messages.

The underlying purpose of Section 14 is to prevent the substantial harms caused by spam on wireless devices and to provide a higher degree of protection to wireless subscribers. To achieve these goals, the Commission must implement the Act in a manner consistent with Congress's intent.

First, Congress was clear on the types of wireless messages the Act was intended to address. The provisions of Section 14 apply only to commercial e-mail messages that are sent directly to a wireless device using the standard two-part address, *e.g.*, NAME@wirelesscarrier.net.[8/] The Act was not expected to apply to short messaging service messages or other short messages that are not sent using the standard two-part address. Likewise, the Act clearly contemplates that wireless carriers could be permitted to send messages to their customers with opt-out consent given the relationship between subscribers and carriers.[9/] Carrier-customer messages simply do not present the same concerns as messages wireless subscribers might otherwise receive from unknown third parties.

Second, Congress intended for consumers to provide their "express prior authorization" to senders in order to receive wireless messages from that sender.[10/] "[R]eflect[ing] the fact that spam to a mobile phone is more intrusive to consumers,"[11/] this provision was clearly intended to prohibit the sending of wireless commercial mobile messages except to subscribers who first request them. Only messages sent from CMRS providers may be sent without prior express

---

[8/] CAN-SPAM Act, §§ 3(5) (defining "electronic mail address"), (6) (defining "electronic mail message").

[9/] CAN-SPAM Act, § 14(b)(3).

[10/] CAN-SPAM Act, § 14(b)(1).

[11/] 149 CONG. REC. H12195 (daily ed. Nov. 21, 2003) (statement of Rep. Markey).

approval (subject to opt-out consent) under the CAN-SPAM Act. Messages from other senders must be the result of affirmative "opt-in" approval from the wireless subscriber.[12/]

Third, Congress directed the Commission to consider the ability of senders to reasonably determine whether a message is being sent to a wireless device.[13/] There are many "innovative technological solutions to combat spam and to protect consumers,"[14/] and thus, the Commission should refrain from adopting one method for determining whether an e-mail address is associated with a mobile device. Rather, the Commission should allow consumers and providers to choose the option that best satisfies their needs as long as the option allows senders to reasonably determine that the message is being transmitted to a wireless device.

Fourth, Congress recognized that complete compliance with the general requirements of the CAN-SPAM Act may not be feasible in light of the technical characteristics of wireless devices and wireless messaging, and directed the Commission to determine whether such compliance is feasible.[15/] In formulating its rules, the Commission must harmonize both the Act's general requirements for commercial e-mail and the specific Congressional directive to take the "unique technical aspects" of wireless devices into account. CMRS senders and other senders that have obtained prior authorization should be able to satisfy the requirements of the CAN-SPAM Act through the use of a working return e-mail address, with fuller descriptions provided at the time of opt-in, subscription, and in monthly bills.

Finally, the requirements applicable to wireless commercial electronic mail messages are included in CAN-SPAM Act's preemption of "any statute, regulation, or rule of a State or

---

[12/] 149 CONG. REC. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey).

[13/] CAN-SPAM Act, § 14(c).

[14/] 149 CONG. REC. H12194 (daily ed. Nov. 21, 2003) (statement of Rep. Goodlatte).

[15/] CAN-SPAM Act, § 14(b)(3).

subdivision of a State that expressly regulates the use of electronic mail to send commercial messages."[16/] The rationale put forward by Congress for establishing a uniform national policy on spam generally – "the inherently interstate nature of e-mail communications" and the fact that "e-mail addresses do not reveal the State where the holder is located"[17/] – applies with equal if not greater force with respect to wireless spam in light of Congress's determination ten years earlier that wireless services themselves "operate without regard to state lines."[18/] In order to avoid confusion and misunderstanding and prevent the prospect of inconsistent state regulation of wireless spam, the Commission should so expressly provide in the rules it adopts in this proceeding.

I. SECTION 14 OF THE ACT APPLIES ONLY TO CERTAIN TYPES OF WIRELESS MESSAGES

Section 14 of the CAN-SPAM Act applies to mobile service commercial messages ("MSCMs"), which are "commercial electronic mail" messages "transmitted directly to a wireless device that is utilized by a subscriber of commercial mobile service."[19/] By limiting the definition of MSCM to "commercial electronic mail," Section 14 excludes certain text messages that fall outside that definition, such as short messages and so-called "short code" transmissions. The Commission has appropriately recognized the relatively narrow scope of Section 14.[20/]

[16/] CAN-SPAM Act, § 8(b)(1) (affording preemptive effect to "[t]his Act" and not just the generally applicable provisions of the Act); *see also* S. REP. NO. 108-102, at 21 (2003) (noting that state law "expressly regulat[ing] the use of e-mail to send commercial messages" is preempted, including "State law requiring some or all commercial e-mail to carry specific types of labels, or to follow a certain format or contain specified content").

[17/] S. REP. NO. 108-102, at 21-22 (2003).

[18/] H. REP. NO. 103-111, at 260 (1993).

[19/] CAN-SPAM Act, § 14(d).

[20/] *See Notice* ¶¶ 9-10.

A. MSCMs Must Be Commercial Electronic Messages

For an MSCM to be considered a "commercial electronic message," the message must first be "commercial."[21/] Whether a message is commercial is based on the primary purpose of the message.[22/] A message is deemed to be "commercial" if the primary purpose is "the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."[23/] A "transactional or relationship message," by contrast, is not a commercial message[24/] and therefore is not covered by the requirements of the Act generally or by Section 14. While the Act provides little guidance for determining the primary purpose of a message, the Act's legislative history makes clear that transactional or relationship messages cannot be deemed "commercial" merely because they include commercial or promotional material.[25/] Like companies that today include commercial "bill stuffers" with monthly bills, a transactional or relationship message also may include commercial content. By "primary purpose," Congress presumably meant that the message would not be sent but for the need to communicate with the recipient regarding a subject that falls within the definition of transactional or relationship message.

As directed by the Act, the Federal Trade Commission ("FTC") has commenced a proceeding to define the relevant criteria for determining the primary purpose of a message and may expand or narrow the types of messages that do not fall within the definition of

---

21/ *Notice* ¶ 11.

22/ CAN-SPAM Act, § 3(2).

23/ CAN-SPAM Act, § 3(2)(A).

24/ CAN-SPAM Act, § 3(2)(B); *id.* § 3(17) (defining "transactional or relationship message" as one whose primary purpose is, *inter alia*, to facilitate a commercial transaction).

25/ S. REP. NO. 108-102, at 16 (2003).

"commercial."[26/] In that proceeding, the FTC has requested comment on several different interpretations of "primary purpose," including that the commercial content is "more important" than the e-mail's other combined purposes; that the commercial content is "more important" than any other single purpose of the e-mail; that the commercial content is more than incidental to the e-mail; or that the "net impression" of a reasonable observer is that the purpose of the e-mail is commercial.[27/] Under any of these approaches, by analogy, a transactional message could include some commercial content. With respect to MCSMs, just as for any commercial electronic messages, the FTC's determination in this regard should govern.

Second, an MSCM must be an "electronic message" and include a unique electronic mail address consisting of both (1) a unique user name or mailbox and (2) a reference to an Internet domain.[28/] These are Internet e-mail messages sent to an e-mail address a consumer has obtained from its CMRS provider, such as NAME@wirelesscarrier.net, and delivered to consumers on their wireless device via their CMRS provider's network.[29/]

By contrast, short messaging service ("SMS") messages, short code messages, or other types of wireless text messages are not MSCMs because these messages do not reference an Internet domain.[30/] SMS messages are text messages directed to a wireless device using the wireless telephone number assigned to that device. These messages are sent from one mobile device to another mobile device or from a carrier to its subscribers. Similarly, short code messages are common five-digit codes that can be used by any wireless subscriber to send text

---

[26/] *Definitions, Implementation, and Reporting Requirements Under the CAN-SPAM Act*, Project No. R411008, Advanced Notice of Proposed Rulemaking (rel. Mar. 10, 2004) ("*FTC Notice*"); CAN-SPAM Act, §§ 3(2)(C), 3(17)(B).

[27/] *FTC Notice* at 16-17.

[28/] *Notice* ¶ 10; *see also* CAN-SPAM Act, §§ 3(5), (6).

[29/] 149 CONG. REC. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey).

[30/] *Notice* ¶ 15.

messages to a company of his or her choice without using the standard two-part electronic mail address.[31/] Wireless subscribers have used short codes to vote for the next American Idol, to register for prizes, or to receive additional information on certain products.

Rarely, if ever, do SMS or short code messages touch the Internet because there is no Internet domain name associated with these messages. SMS messages can be sent between subscribers of different carriers because the carriers have entered into arrangements with each other that permit such exchanges without the need to use the public Internet. Section 14 and the Act generally are therefore inapplicable to SMS, short code, and other types of wireless text messages because they lack the essential characteristics of electronic messages.[32/]

Even if such messages could be considered MSCMs, there is no need to apply the Act's requirements to them. Wireless carriers have a strong incentive to protect their customers from unwanted messages and are taking the necessary precautions to prevent an explosion of spam on wireless devices similar to that which has invaded the wired Internet. As discussed more fully below, wireless providers have employed technical measures to prevent SMS spam from reaching their customers, such as using spam filters or allowing customers to create lists of permissible senders for receiving messages.[33/] Likewise, carriers have been aggressively pursuing legal actions against third parties that send SMS spam to their customers.[34/]

[31/] Mike Dano, *Carriers Connect on Short Codes*, RCR WIRELESS NEWS (Oct. 20, 2003).

[32/] Given the negligible amount of SMS traffic that traverses the Internet, there is no need to subject the Act's requirements to those rare cases in which SMS messages are first sent through the Internet and then converted into an SMS message associated with a telephone number.

[33/] *ContentCatcher Now Supports BlackBerry and 3G Wireless*, MARKET WIRE (Feb. 5, 2004) (discussing new mobile spam filters); *see also infra* Section III.

[34/] Nextel, for example, has filed two such suits against known wireless spammers. *See, e.g.*, *Nextel Communications, Inc. v. Enyo Communications*, Complaint (N.D. Ga. Feb. 2004); *Nextel Communications, Inc. v. Edwards*, Complaint (N.D. Ga. Apr. 21, 2004); *see also infra* Section III.

Moreover, SMS or short code spam simply does not present the same concerns as electronic messages sent over the Internet. Because carriers typically charge a per-message fee for mobile originated messages, the economics of using a mobile network to send spam messages is entirely different from the Internet model. The architecture of the wireless network also gives wireless carriers a level of control that is not available on the Internet, which provides a further deterrent to spam.[35/] SMS and short code messages go through a carrier owned and controlled gateway to reach wireless customers. The gateway is designed to facilitate the transmission of individual messages addressed to a wireless phone number. They do not support multiple messages and are designed to detect and filter multiple identical messages or services are available to do so.[36/] While it is possible to send SMS spam to wireless users one or two messages at a time, the process is so cumbersome that it has not become as problematic as Internet-based messages.[37/]

Further, wireless carriers typically do not market their subscriber lists to third parties, and wireless numbers are not posted throughout the Internet like Internet-based electronic mail addresses. This makes it much more difficult for spammers to obtain the "addresses" (*i.e.*, wireless telephone numbers) for unsolicited SMS messages. For all of these reasons, there is no basis or rationale for the Commission to include SMS messages within the requirements of Section 14.[38/]

[35/] Michelle Megna, *Mobile Users Pounded by Marketers, Junk Mail Pay Price*, DAILY NEWS (July 10, 2003) (noting that "cell phone use does not have the public-access concerns of the Internet," and thus, wireless providers are "able to use a range of tools to protect consumers' privacy").

[36/] Thus, while spammers can randomly generate numbers for the number field in a typical wireless address, *i.e.* NPA-NXX-XXXX@wirelesscarrier.net, such messages would be blocked.

[37/] Mike Dano, *Text Messaging Spam Nearly Non-Existent*, RCR WIRELESS NEWS (June 17, 2002).

[38/] Additionally, the Commission has held that unsolicited SMS is covered by the Telephone Consumer Protection Act ("TCPA"). *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd 14014, ¶ 165 (2003) ("*2003 TCPA Order*"); *see also Notice* ¶ 15. CTIA takes no position as to the correctness of that determination.

B. MSCMs Must Be Transmitted Directly to a Wireless Device

CTIA also supports the Commission's determination that messages must be "transmitted directly to a wireless device used by a subscriber of commercial mobile service" in order to be deemed an MSCM under the Act.[39/] As the Commission suggests, the specific transmission technique used to deliver the message to the wireless device is not relevant to the inquiry.[40/] Rather, the relevant consideration is whether the message is sent *directly* to the wireless device and intended to be sent to the wireless device.

The requirements of Section 14 should not apply to "forwarded" messages, such as those used on "Blackberry" devices.[41/] As the Commission acknowledges, forwarded messages are not "transmitted directly to a wireless device" because they are not intended to be received on the wireless device.[42/] Rather, subscribers must take affirmative action to have messages forwarded to the wireless device. Moreover, senders could not be held liable for sending unauthorized MSCMs if subscribers are permitted to convert non-MSCMs into MSCMs without the sender's knowledge.[43/] The legislative history of the CAN-SPAM Act indicates that the definition of electronic mail message was "intended to apply to the message in the form that it is sent, regardless of whether or in what form it is received."[44/] In addition, because these types of messages are initially sent to an electronic mail account that is normally accessed by a personal computer, the Act's general requirements would apply to these types of messages.[45/] Including forwarded messages in the definition of MSCM would improperly expand Section 14 to cover all

---

[39/] *Notice* ¶ 12.

[40/] *Notice* ¶¶ 12, 14.

[41/] *Notice* ¶ 16.

[42/] *Notice* ¶ 16.

[43/] *Notice* ¶ 17.

[44/] S. REP. NO. 108-102, at 14 (2003).

[45/] 149 CONG. REC. H12196 (daily ed. Nov. 21, 2003) (statement of Rep. Markey).

electronic mail rather than just that electronic mail specifically intended to be sent to a wireless device.

II. THE CAN-SPAM ACT REQUIRES ALL NON-CMRS SENDERS TO OBTAIN PRIOR AUTHORIZATION TO SEND MESSAGES TO WIRELESS SUBSCRIBERS

A. Wireless Subscribers Should Be Required To Take Affirmative Action To Receive MSCMs from Senders other than their Wireless Provider

Under the requirements of the CAN-SPAM Act, subscribers must be provided the "ability to avoid receiving [MSCMs] unless the subscriber has provided express prior authorization to the sender."[46/] Thus, the plain language of the Act requires that subscriber consent to receive MSCMs must occur *prior* to the receipt of any such messages and it must be *express*.[47/] This regime is distinct from the "opt-out" structure applicable to other commercial electronic mail messages, under which a sender may send an initial message provided that the message includes a mechanism that the recipient can use to prevent any additional messages.

Congress intended wireless subscribers to have greater protections than other recipients of commercial e-mail because there is a substantial interest in ensuring that wireless subscribers do not receive unwanted messages.[48/] Not only do subscribers face per-message fees for unwanted MSCMs, but an influx of MSCMs can overwhelm both subscribers and the wireless network itself. Given Congress's strong interest in protecting wireless subscribers, senders (except for CMRS senders as discussed below) should be prohibited from sending MSCMs unless and until the wireless subscriber gives her express prior authorization to receive the MSCM from that sender as required by the Act.

[46/] CAN-SPAM Act, § 14(b)(1).

[47/] *Notice* ¶ 21.

[48/] 149 CONG. REC. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey).

CTIA agrees that the Act's definition of "affirmative consent" would be an appropriate touchstone for defining "express prior authorization."[49/] In the wireless context, express prior authorization means that consumers must "opt-in" to receive MSCMs.[50/] This is similar to the intent underlying "affirmative consent," which requires "some kind of active choice or selection" rather than "merely remaining passive, as in the case where a consumer fails to modify a default setting expressing consent."[51/]

The Commission should not adopt a particular format or dictate particular requirements for wireless subscribers to provide their express prior authorization.[52/] Rather, any indication evidencing the subscriber's affirmative desire to receive the MSCM from the sender should be sufficient. Senders should not be permitted to use "negative options" or other devices that do not require action on the part of the subscriber to authorize the sender to transmit MSCMs to the subscriber.[53/]

In addition, subscribers should be given the flexibility to provide their consent through a variety of methods, either via the Internet, over the phone, or from their wireless device. Authorization should not be required in writing,[54/] but senders should be required to keep records

---

[49/] *Notice* ¶ 35.

[50/] 149 CONG. REC. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey); 149 CONG. REC. 12195 (daily ed. Nov. 21, 2003) (statement of Rep. Markey).

[51/] S. REP. NO. 108-102, at 13 (2003). The Commission should likewise make clear that consent is presumed to continue until the recipient takes affirmative action to revoke it. While this may occasionally result in an MSCM being sent to a wireless number that has been reassigned to a person other than the one who gave consent, it is no more of a burden on that person that the inconvenience of receiving a call intended for the former subscriber.

[52/] *Notice* ¶¶ 35-36.

[53/] The use of a negative option to obtain consent has been looked at with disfavor by the Commission. *See, e.g.*, *Investigation of Access and Divestiture Related Tariffs*, 101 FCC 2d 911 (1985) (default options are against the public interest because they confer advantages on the company making the negative option).

[54/] *Notice* ¶ 35.

of written, electronic, and oral authorizations for at least one year.[55/] Likewise, senders should have the ability to tailor the format and content of the consent to fit their individual business models, the wireless device used, or the subscriber's preferences. The Commission has taken a similar approach in its carrier change authorization rules, which allow carriers to obtain consumer consent orally, in writing, or through the use of a third party verifier to change service providers.[56/] The Commission recognized that providing carriers with options for obtaining consent struck a balance between protecting consumers and promoting competition.[57/]

The Commission should not exempt small businesses sending MSCMs to wireless subscribers from the prior express authorization requirement.[58/] There is no support in the Act for such an exemption. The permitted exception to the Act's prior authorization requirement is for MSCMs sent to wireless subscribers by their wireless provider as discussed below.[59/] Allowing small businesses to send MSCMs without prior authorization would undermine the Act's goals to protect consumers, especially wireless subscribers, from unwanted messages. Wireless subscribers need to be protected from unknown senders of all sizes. Any other action would risk creating a huge loophole for spammers. Given the small amount of capital required to send literally millions of spam messages (as policymakers have recognized, spam messages

---

[55/] This is consistent with the record retention requirements for consents to use customer proprietary network information ("CPNI"). 47 C.F.R. § 64.2009(c).

[56/] 47 C.F.R. § 64.1120.

[57/] *Implementation of the Subscriber Carrier Selection Changes Provisions of the Telecommunications Act of 1996; Policies and Rules Concerning Unauthorized Changes of Consumers Long Distance Carriers*, Second Report and Order and Further Notice of Proposed Rulemaking, 14 FCC Rcd 1508, ¶ 16 (1998).

[58/] *Notice* ¶¶ 23, 36.

[59/] CAN-SPAM Act, § 14(b)(3).

are virtually costless to the sender) small companies will take advantage of any exception in the spam rules.[60/]

B. CMRS Providers Should Be Exempted from the Requirement To Obtain Express Prior Approval before Sending Messages to their Customers

Although the CAN-SPAM Act requires CMRS subscribers to give their express prior authorization to a sender before receiving an MSCM,[61/] the Act also directs the Commission to determine whether CMRS providers should be exempt from the prior authorization requirement when sending MSCMs to their own subscribers.[62/] CTIA supports such an exemption for CMRS providers.[63/]

Wireless carriers routinely communicate with their customers regarding new offers, the availability of upgraded services or products, special discounts, or service reminders,[64/] and subscribers benefit from the availability of this information. In creating an exception to the express prior authorization requirement for MSCMs from carriers to subscribers, Congress recognized that it would be reasonable for the Commission to facilitate such communications via commercial electronic messages sent directly to wireless handsets.[65/] Many of these types of messages would not fall within the definition of "transactional or relationship message" under the CAN-SPAM Act[66/] but would nonetheless provide useful and beneficial information to

---

[60/] Because the cost of spam is borne almost entirely by the recipient, it is particularly attractive to fly-by-night small businesses promoting dubious products.

[61/] CAN-SPAM Act, § 14(b)(1).

[62/] CAN-SPAM Act, § 14(b)(3).

[63/] *Notice* ¶ 39.

[64/] *Notice* ¶ 39.

[65/] *See* CAN-SPAM Act, § 14(b)(3) (directing the Commission to "take into consideration . . . the relationship that exists between providers of [commercial mobile] services and their subscribers" in determining whether to establish an exemption to the express prior authorization requirement). Note that wireless carriers, like any other sender of commercial electronic mail messages, can send an initial message to a customer's PC (or any person's PC) without express prior consent.

[66/] CAN-SPAM Act, § 3(17).

wireless subscribers.[67/] There are many such messages, including announcements of new rate plans that may save the customer money, new features, or services offering substantial convenience to the customer such as traffic alerts.

Unlike senders without any relationship to the recipient, CMRS providers have strong market incentives not to abuse their relationships with wireless subscribers.[68/] As the Commission has noted on numerous occasions, the CMRS industry is robustly competitive. Nearly 95 percent of the total population of the United States have three or more competitive alternatives for wireless service and 71 percent of the population have six or more choices among providers.[69/] With the advent of local number portability and the myriad of competitive wireless plans available today, no wireless carrier will risk alienating a subscriber by sending unnecessary, unwanted, or irrelevant messages. Any possible inconvenience to consumers also is negated by the Act's directive that wireless subscribers be permitted to "opt-out" of receiving messages when they subscribe to the wireless service or via a billing mechanism.[70/] Indeed, several carriers already have established opt-out policies and routinely inform their customers of their ability to opt-out of receiving messages from their wireless carrier.

While this requirement will ensure that wireless subscribers do not receive unwanted MSCMs from their carriers, CTIA proposes that, instead of adopting a specific mechanism for "opt-outs," the Commission should allow wireless subscribers to indicate that they no longer wish to receive carrier MSCMs through a variety of methods. For example, subscribers could

---

67/ *Notice* ¶ 39.

68/ *Cf.* 47 U.S.C. § 227(b)(2)(C) (exempting autodialed calls from a wireless carrier to its subscribers from the general prohibition on such calls to cellular telephone numbers); 47 C.F.R. § 64.1200(a)(1)(iii) (same).

69/ *Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions With Respect to Commercial Mobile Services*, Eighth Report, 18 FCC Rcd 14783, ¶ 84 (2003).

70/ CAN-SPAM Act, § 14(b)(3); *see also Notice* ¶ 40.

notify the carrier by calling the carrier's customer service representative, mark a check-box on a written contract when purchasing service, or opt-out via the Internet or a message (SMS or e-mail) sent from their wireless device. Giving consumers the flexibility to decline provider messages in any number of ways would benefit the public interest by allowing consumers to control the terms of their carrier-customer relationships.

In addition, the exemption for CMRS providers should encompass all messages sent to subscribers regarding the family of services offered by the wireless provider.[71/] As under the Commission's CPNI rules for wireless services, wireless carriers should be permitted to send messages to their subscribers that the customer reasonably expects to receive based on the services it purchases from the wireless provider.[72/] Under such an approach, wireless providers would be permitted to send messages regarding enhancements to a subscriber's current service or to explain new features of a service without the subscriber's express prior permission.[73/] As the Commission has recognized in the CPNI context, consumers reasonably expect the service providers with whom they deal to advise them about new or additional features, functions, equipment, or service offerings that can be bundled with existing services or equipment, save the consumer money, or provide other consumer benefits.[74/]

[71/] *Notice* ¶ 39.

[72/] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶ 17 (1999).

[73/] CMRS carriers also should be permitted to send their customers wireless e-mail regarding partner offerings. Carriers have the same incentives not to alienate their customers with unwanted commercial e-mail, regardless of the content of the message.

[74/] *See, e.g.*, *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order, 17 FCC Rcd 14860, ¶ 36 (2002); Order on Reconsideration, 13 FCC Rcd 8061, ¶¶ 41, 43 (1999).

III. THE COMMISSION SHOULD NOT DICTATE A SPECIFIC METHOD OR TECHNOLOGY FOR DETERMINING WHETHER MESSAGES ARE MSCMs

CTIA agrees with the Commission that there could be "a variety of mechanisms" for senders to determine whether they are sending a message to a wireless subscriber or for protecting wireless subscribers from unwanted MSCMs.[75/] The Commission, however, should not dictate any one technology or strategy for eliminating wireless spam and should not disturb the procedures wireless providers currently are using today. Rather, the Commission should allow consumers and wireless carriers to choose the option that best fits their needs. Consumers and their providers "can do far more to protect the nation's inboxes from unsolicited e-mail than any law."[76/]

Wireless providers have already gotten aggressive against spam. Several carriers have filed lawsuits against spammers sending unsolicited and unwanted messages to their subscribers. Nextel, for example, has filed two suits against wireless spammers who each sent hundreds of thousands of messages to Nextel customers.[77/] Others have exercised their rights to suspend or rescind handset contracts with companies identified as spammers. For example, as of November 2003, NTT DoCoMo has suspended 1875 contracts because of spamming.[78/]

Several wireless providers also have implemented software programs that monitor e-mail to eliminate spam or allow their customers to create lists of senders from which messages will, or will not, be accepted. Most of these programs allow either the carrier or the subscriber (or both)

[75/] *Notice* ¶¶ 19, 25.

[76/] 149 CONG. REG. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Sensenbrenner).

[77/] Because the conduct at issue in these suits preceded enactment of the CAN-SPAM Act, the ISP right of action under the Act, CAN-SPAM Act, § 7(g), was not available to Nextel. Nextel and other CMRS providers will be able to bring actions under Section 7(g) as well as under state trespass and conversion laws that were expressly preserved by the Act. CAN-SPAM Act, § 8(b)(2)(A).

[78/] Susan Rush, *NTT DoCoMo: Spam, Spam Go Away*, WIRELESS WEEK (Nov. 5, 2003).

to administer rules to define the level of content filtering on incoming messages.[79/] These programs intercept messages and filter them based on the individual subscriber's preferences. Other carriers have installed blocking features, which allow users to automatically reject messages from a sender that sends more than a certain pre-set number of messages per day. Subscribers generally have the ability to turn off the anti-spam features if they wish. In addition, at least one carrier has introduced new handsets that enable subscribers to check the subject line of an incoming e-mail prior to downloading it.[80/]

Although wireless providers as carriers generally have the right under their customer contracts as well as Federal law to "protect their rights or property,"[81/] the Commission should expressly acknowledge a "safe harbor" for CMRS providers that filter or block wireless spam whether or not at the request of a subscriber. A safe harbor would limit CMRS providers' liability for blocking or filtering legitimate messages that the provider reasonably believed in good faith to be spam. Congress has recognized similar protections for Internet service providers ("ISPs") under Section 230 of the Communications Act,[82/] and has made clear that nothing in the CAN-SPAM Act affects ISPs' policies for blocking or filtering spam.[83/] When CMRS providers intercept and filter spam at the request of their customers or to protect their rights or property, they are acting like ISPs that take the same actions with respect to spam sent to personal computers. CMRS providers are under no obligation to provide these protections, but do so for

---

79/ Emily Motsay, *Trash or Treasure: Industry Takes on Wireless Spam*, RCR WIRELESS NEWS (July 7, 2003).

80/ John L. Guerra, *Wireless Spam: Coming to a Cell Phone Near You?*, BILLING WORLD AND OSS TODAY (March 2004).

81/ Electronic Communications Privacy Act, 18 U.S.C. § 2702.

82/ 47 U.S.C. § 230.

83/ CAN-SPAM Act, § 8(c).

the benefit of their customers and to protect their networks and e-mail services against a deluge of mail that may cripple or degrade their service offerings.

In their capacity as providers of electronic messaging and other information services, many wireless providers have terms of service, acceptable use, and privacy policies that inform customers of the carrier's blocking procedures and standards. They also have posted policies that inform third parties that sending spam to customers is unauthorized. There is no reason CMRS carriers should not be provided the same protections as other entities that block or filter spam for their customers. The CAN-SPAM Act, however, does not provide a basis for the Commission to impose particular network or other requirements on CMRS providers in their capacity as carriers.[84/] As a general matter, the Act's obligations are imposed on senders of commercial electronic messages. Entities that engage in "routine conveyance" of such messages are expressly not considered senders.[85/]

To the extent the Commission seeks to adopt a specific mechanism for prohibiting the sending of unauthorized MSCMs, CTIA supports the creation of a specific wireless domain name to be used for wireless subscribers.[86/] To facilitate this process, the Commission could request a specific high-level domain name from the Internet Corporation for Assigned Names and Numbers ("ICANN") to be used for wireless subscribers (such as .air). Wireless subscribers, however, should not be required to use such a domain name if they choose not to. Rather, subscribers should be permitted to decline to use the domain name and accept the possible risk of receiving spam. As discussed above, consumers also should have the flexibility to choose the

---

[84/] 149 CONG. REC. H12860 (daily ed. Dec. 8, 2003) (statement of Rep. Markey) ("wireless carriers should not see [] burdens implemented as part of Section 14 to the extent to which they are acting as carriers").

[85/] CAN-SPAM Act, § 3(16) ("sender" means a person who "initiates" a commercial electronic mail message); *id.* § 3(9) (excluding "actions that constitute routine conveyance of such message" from the definition of initiate).

[86/] *Notice* ¶ 30.

appropriate anti-spam mechanism offered by their carrier that best suits the consumer's individual needs.

In addition, even with the creation of a wireless-specific domain name, non-CMRS senders should still be required to obtain prior express approval from wireless subscribers before sending MSCMs. The burden is on the sender to determine whether the recipient has given her express approval to receive MSCMs from the sender – the assignment of a wireless-specific domain name in no way changes the Act's requirements that senders obtain prior express authorization. Use of the wireless-specific domain name is merely a mechanism for a sender to know that it needs prior approval to send the message because it is sending the message to a wireless device.

In comparison to the other alternatives proposed by the Commission, use of a wireless-specific domain name is the most efficient and practicable method for informing senders that messages are being sent to a wireless device, and will result in the least burden on wireless subscribers and providers. By contrast, a challenge-and-response system, which sends back a challenge that requires a response verifying some aspect of the message, would increase the number of messages wireless subscribers receive, thereby increasing costs if customers are billed per-message,[87/] and cause additional congestion on wireless networks.[88/] Likewise, the creation of registry of individual subscriber addresses could have the unintended consequences of giving spammers that choose to ignore the law a complete listing of wireless addresses that could be used to generate more spam.[89/] Accordingly, the Commission should allow, but not require, the

---

[87/] The cost of defending against unwanted messages should not be transferred to either the customer or the service provider.

[88/] *Notice* ¶ 32.

[89/] *Notice* ¶ 29; *see also Hayward Firm Sued over Do-Not-Call List*, SAN FRANCISCO BUSINESS TIMES (Nov. 7, 2003); *Florida Telemarketer Sued for Violating 'Do Not Call' List* (Sept. 4, 2003), *available at* http://www.local6.com/print/2454725/detail.html?use=print.

use of a wireless-specific domain name in addition to the other anti-spam techniques currently being implemented by wireless providers.

IV. THE COMMISSION SHOULD TAKE THE UNIQUE TECHNICAL CHARACTERISTICS OF WIRELESS DEVICES INTO CONSIDERATION IN DETERMINING HOW SENDERS OF MSCMs MAY COMPLY WITH THE PROVISIONS OF THE ACT

Regardless of any authorization supplied by the recipient, the CAN-SPAM Act requires specific information to be included in all commercial e-mail messages, such as header information, a valid return e-mail address, identifiers for certain content, a mechanism to opt-out of receiving future messages, and a physical postal address.[90/] The purpose of these provisions is to ensure that consumers know what entity is sending the message and how to stop receipt of future messages. Congress recognized, however, that it would be impractical and, in some cases, impossible, for senders of MSCMs to comply with all of the Act's requirements, and it therefore directed the Commission to consider alternatives.[91/]

As the Commission recognizes, the character limitation on text messages means that including the required information in MSCMs could reduce the length of the substantive message given the character limitations for most wireless messages.[92/] Additionally, some handsets do not have the memory capabilities to send, receive, and store messages beyond certain lengths. Moreover, many handsets require multiple keystrokes to enter alphanumeric data using the traditional telephone key pad, and lack a "QWERTY" keyboard that would facilitate a recipient's ability to respond to a message. Finally, the small screen size of most wireless devices creates a "functional limitation" on the ability to display the complete text of a longer message..

[90/] CAN-SPAM Act, § 5.

[91/] CAN-SPAM Act, § 14(b)(4); *Notice* ¶ 41.

[92/] *Notice* ¶ 42.

Accordingly, the Commission should find that the requirement for a "clear and conspicuous display" of an opt-out mechanism is satisfied by the availability in an MSCM of a working e-mail address to which consumers could opt-out of receiving future messages. Because of their business relationship with their carrier, wireless subscribers know the identity of the entity sending the message, how to contact that entity, and how to stop the receipt of additional messages. Consumers would also have a similar relationship with other senders of MSCMs since those senders must first obtain the customer's express prior authorization before sending the message.

As required by Section 14, wireless carriers exempted from the express prior authorization requirement must provide the information required by Section 5 of the Act at the time of subscription and in each monthly bill.[93/] The Commission should also require other authorized senders of MSCMs to provide this information in full at the sender's website, in a non-MSCM electronic message to the recipient, through conventional mail, or some combination of the foregoing. Such an approach would harmonize the requirements of the Act while ensuring that wireless subscribers receive the heightened protections envisioned by Congress.

CONCLUSION

For the foregoing reasons, CTIA asks the Commission to adopt its tentative conclusion that only certain wireless messages fall within the scope of Section 14 of the CAN-SPAM Act, and accordingly, find that SMS, short code, and other text messages are not subject to the Act's requirements. CTIA also requests that the Commission determine that CMRS providers are

---

[93/] CAN-SPAM Act, § 14(b)(3)(A), (B). Interpreting the statutory directive that CMRS providers "comply[] with the other provisions of [CAN-SPAM]" to mean that all of the information mandated by Section 5 of the Act be included in every MSCM would render Section 14(b)(4) meaningless. It is a fundamental principle of statutory construction that a law should be interpreted so as to give effect to each provision. *See, e.g., South Carolina v. Catawba Indian Tribe, Inc.*, 476 U.S. 498, 510 n.22 (1986) (noting the "elementary canon of construction that a statute should be interpreted so as not to render one part inoperative.") (quoting *Colautti v. Franklin*, 439 U.S. 379, 392 (1979).

exempt from the obligation to obtain prior express approval before sending MSCMs. The Commission, however, should require wireless subscribers to take affirmative action in order to receive MSCMs from non-CMRS senders. In addition, the Commission should not disturb the anti-spam mechanisms currently used by carriers or adopt one particular method for determining whether messages are being sent to wireless devices. Finally, the Commission should take the unique characteristics of wireless devices into account when determining how senders of MSCMs may comply with the Act's general requirements for all commercial e-mail.

Respectfully submitted,

/s/ Michael Altschul

CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION

Howard J. Symons
Angela F. Collins
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004
(202) 434-7300

Of Counsel

Michael F. Altschul
Senior Vice President and General Counsel
CELLULAR TELECOMMUNICATIONS & INTERNET ASSOCIATION
1400 16th Street, N.W.
Suite 600
Washington, D.C. 20036
(202) 785-0081

April 30, 2004